(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 13/00

(11) 공개번호 특2002-0088540
(43) 공개일자 2002년11월29일

(21) 출원번호 10-2001-0027242
(22) 출원일자 2001년05월18일

(71) 출원인 아라리온 (주)
서울 서초구 서초2동 1330-3번지 ASIC벤처타운 10층

(72) 발명자 정자춘
서울특별시강동구고덕동584-9

이평한
경기도성남시분당구정자동한솔주공609동1904호

엄재홍
서울특별시광진구모진동210-23F

최훈규
경기도성남시분당구수내동73벽산아파트306동1103호

주유진
10119사우스블라니에이브이이.쿠퍼티노캘리포니아95014미합중국

황태용
1556해포드에이브이이#220산타클라라,캘리포니아95051미합중국

김용원
3567벤톤스트리트.#303산타클라라,캘리포니아95051미합중국

(74) 대리인 박원용, 이증우

심사청구 : 있음

(54) 이중버스를 연결하는 고기밀 호스트 어댑터

요약

본 발명은 이중버스를 연결하는 고기밀 호스트어댑터에 관한 것으로서, 그 목적은 컴퓨터의 외부접근자의 요구에 의해 컴퓨터 내에 내장된 정보를 외부로 전송 또는 외부접근자가 정보를 컴퓨터 내에 저장하려할 때 암호화하여 전송되어진 정보를 복호화하고, 복호화된 정보를 암호화하여 저장하도록 하며, 암호화 및 복호화시 다른 버스를 점유하지 않고 어댑터 내부에서 처리하므로 용량 및 속도를 개선하도록 하며 네트워크에 연결된 저장장치의 저장된 정보를 인증된 인원에게만 제공하는데 있다.

본 발명의 목적은 이중버스를 연결하는 고기밀 호스트어댑터는 컴퓨터의 시스템 메모리 또는 중앙처리장치와 인터페이스하는 제 1 버스와, 하드디스크의 데이터의 읽기/쓰기를 수행하는 상기 제 1 버스와 다른 방식의 제 2 버스와, 상기 제 1 버스와 제 2 버스 간의 데이터를 인터페이스하는 어댑터와, 상기 어댑터의 동작제어를 위한 프로그램이 등록된 롬바이오스로 구성된 이중버스간의 어댑터에 있어서, 제 1 버스에 접속된 마스터컨트롤러와 하드디스크간에 전송되는 데이터를 쓰기/읽기에 따라 제공된 비밀키 데이터에 의하여 암호화/복호화하는 제 1 암/복호화수단과, 제 1 암/복호화수단 및 다른 암/복화수단으로부터 입출력되는 데이터를 선입선출 버퍼링하는 선입선출버퍼와, 상기 선입선출버퍼를 통해 선입선출되는 데이터를 하드디스크로의 쓰기/읽기 동작에 따라 암호화/복호화하여 제 2 버스로 전송하는 제 2 암호화/복호화수단과, 상기 제 1, 제 2 암/복호화수단의 암호화 또는 복호화를 결정하여 인에이블시킴과 아울러 암호화 및 복호화할 비밀키 데이터를 제공하는 암/복호화제어수단으로 이루어짐을 특징으로 한다.

대표도

도2

색인어

이중버스, 암호화, 복호화, 비밀키, 선입선출 버퍼, FIFO, 하드디스크

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 이중버스를 연결하는 고기밀 호스트어댑터를 설명하기 위한 개략 구성도이고,

도 2는 본 발명의 실시예에 따른 이중버스를 연결하는 고기밀 호스트어댑터의 상세 블록 구성도이다.

< 도면의 주요부분에 대한 부호의 설명 >

100 : 호스트 어댑터110 : PCI 인터페이스부

111 : 마스터 컨트롤러12 : 슬레이브 컨트롤러

120, 130 : 제 1, 제 2 암호화/복호화 처리장치

121, 131 : 제 1, 제 2 암/복호화부

122 : 선입선출버퍼140 : IDE 인터페이스부

150 : 암/복호화 제어부

151, 153 : 제 1, 제 2 암/복호화구동부

152 : 비밀키 제어부162 : 롬 인터페이스부

200 : 롬 바이오스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 컴퓨터 내의 이중 버스간을 상호연결하는 어댑터에 관한 것으로서, 보다 상세하게는 PCI(Peripheral Component Interconnect), IDE(Integrated Devices Electronics) 또는 SCSI(Small Computer System Interconnection)방식의 버스 상호간을 연결하도록 하고, 어댑터 내부에 암호화 및 복호화 기능을 동시에 진행할 수 있도록 하여 고기밀성을 유지하며, 저가로 설치가능하며, 유지보수가 쉽고 간단하도록 하는 이중버스를 연결하는 고기밀 호스트어댑터에 관한 것이다.

최근 인터넷 속도의 비약적인 발전과 개인용컴퓨터(PC)와 산업용컴퓨터(Workstation)를 하나의 네트워크로 연결시키고 있다. 회사와 회사의 연결(Extranet), 회사내의 부서간의 연결(Intranet), 각 가정 및 영업현장에서 회사의 산업용컴퓨터와 연결할 수 있는 기술(VPN:Virtual Private Network) 등이 제공되고 있다.

그러나, 이러한 네트크워들은 인터넷에 노출되어 있기 때문에 산업정보의 불법 유출하는 폐단이 발생하여 기업의 손실을 발생하고 있다. 이를 방지하기 위하여 고가의 고성능 네트워크 장비를 구비하여야 하는 문제점이 있으며, 이의 유지보수또한 많은 비용과 인력이 소요되어야 한다.

또한, 컴퓨터용 저장장치의 용량이 점차 거대화되고, 액세스 속도도 점차 고속화 되어가고 있다. 이러한 컴퓨터용 저장장치 역시 네트워크에 직접 연결되어 있으므로 저장된 정보유출의 위험성에 노출되어 있다.

이와 같은 저장장치로 ATAPI(AT Attachment with Packet Interface)기술을 이용한 IDE(Integrated Devices Electronics)용 저장장치와 SCSI(Small Computer System Interconnection)용 저장장치가 있다. SCSI용 저장장치는 전송속도나 안정성면에서 IDE용 저장장치보다 우수하다.

암호화 기술 또는 알고리즘은 크게 2가지로 분류되는데, 첫째는 개인키(Private key), 공개키(Public key)의 서로 다른 키시스템(Key system)을 이용하여 암호화 내지 복호화를 수행하는 비대칭 암호화(Asymmetric cryptosystem) 또는 PKI(Public Key Infrastructure) 시스템이 있다. PKI의 대표적인 알고리즘은 'RSA'인데, 주로 개인 대 개인(Peer to Peer)통신수단에 있어 우수한 도구고 사용되고 있다.

둘째는 암호화, 복호화 수행에 동일한 키를 사용하는 대칭암호화(Symmetric cryptosystem)이다. 대표적인 알고리즘은 'IDEA 와 DES'이며, 암호화와 복호화에 동일한 키를 사용하기 때문에 암호화된 문서나 정보를 복호화하기 위해 송신 시 키를 같이 수신자에게 전달하여야 한다. 또한 서로 다른 알고리즘은 키를 분석하는 방식이 다르기 때문에 상호호환이 되지 않는다. 암호화 기술은 하드웨어로도 구현이 가능하나 다른 알고리즘을 적용할 경우 호환이 매우 어렵다. 또한, 각 컴퓨터가 접속된 ISP(Internet Service Provider)의 통신 장비와의 호환을 고려하여야 하며, 호환이 보장된다 하더라도 각 가정이나 영업현장에서 게이트웨이(gateway)와 같은 통신장비까지의 연결에서 비밀이 보장되지 않고 정보가 노출되는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 종래기술의 제반 문제점을 해결하기 위한 것으로, 그 목적은 컴퓨터의 외부접근자의 요구에 의해 컴퓨터 내에 내장된 정보를 외부로 전송 또는 외부접근자가 정보를 컴퓨터 내에 저장하려할 때 암호화하여 전송되어진 정보를 복호화하고, 복호화된 정보를 암호화하여 저장하도록 하며, 암호화 및 복호화시 다른 버스를 점유하지 않고 어댑터 내부에서 처리하므로 용량 및 속도를 개선하도록 하며 네트워크에 연결된 저장장치의 저장된 정보를 인증된 인원에게만 제공하도록 하는 이중버스를 연결하는 고기밀 호스트어댑터를 제공함에 있다.

발명의 구성 및 작용

본 발명의 목적을 달성하기 위한 본 발명에 따른 이중버스를 연결하는 고기밀 호스트어댑터는 컴퓨터의 시스템 메모리 또는 중앙처리장치와 인터페이스하는 제 1 버스와, 하드디스크의 데이터의 읽기/쓰기를 수행하는 상기 제 1 버스와 다른 방식의 제 2 버스와, 상기 제 1 버스와 제 2 버스 간의 데이터를 인터페이스하는 어댑터와, 상기 어댑터의 동작제어를 위한 프로그램이 등록된 롬바이오스로 구성된 이중버스간의 어댑터에 있어서, 상기 제 1 버스에 접속된 마스터컨트롤러와 하드디스크간에 전송되는 데이터를 쓰기/읽기에 따라 제공된 비밀키 데이터에 의하여 암호화/복호화하는 제 1 암/복호화수단과, 상기 제 1 암/복호화수단 및 다른 암/복화수단으로부터 입출력되는 데이터를 선입선출 버퍼링하는 선입선출버퍼와, 상기 선입선출버퍼를 통해 선입선출되는 데이터를 하드디스크로의 쓰기/읽기 동작에 따라 암호화/복호화하여 제 2 버스로 전송하는 제 2 암호화/복호화수단과, 상기 제 1, 제 2 암/복호화수단의 암호화 또는 복호화를 결정하여 인에이블시킴과 아울러 암호화 및 복호화할 비밀키 데이터를 제공하는 암/복호화제어수단을 포함하여 이루어짐을 특징으로 한다.

여기서, 암/복호화제어수단은 상기 제 1, 제 2 암/복호화수단에 현재 입력된 데이터의 암호화/복호화 여부를 접속 요청자의 인증여부에 따라 결정함과 아울러 해당 비밀키 데이터를 저장 및 제공하는 비밀키 제어수단과, 상기 비밀키 제어수단으로부터 전송된 비밀키 데이터와 제 1, 제 2 암/복호화수단 제어신호에 따라 해당 암/복호화수단을 인에이블 시킴과 아울러 비밀키 데이터를 제공하는 제 1, 제 2 암/복호화 구동수단으로 이루어짐을 특징으로 한다.

이와 같이 이루어진 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다.

도 1은 본 발명의 일 실시 예에 따른 이중버스를 연결하는 고기밀 호스트어댑터를 설명하기 위한 개략 구성도로서, 이에 도시된 바와 같이 시스템 메모리 또는 중앙처리장치(CPU)와 접속된 PCI 버스의 데이터를 인터페이스하는 PCI버스 인터페이스(110)와, 상기 PCI버스 인터페이스(110)에 입출력되는 데이터를 현재 IDE 하드디스크를 액세스하고 있는 사용자의 비밀키(Key1)에 의하여 암호화 또는 복호화하는 제 1 암호화/복호화처리부(120)와, 네트워크를 통하여 하드디스크를 엑세스하는 사용자의 비밀키(Key2)에 의하여 상기 제 1 암호화/복호화처리부(120)에서 전송된 복호화된 데이터를 암호화하거나 하드디스크에서 암호화되어 저장된 데이터를 복호화하는 제 2 암호화/복호화처리부(130)와, 상기 제 2 암호화/복호화처리부(130)와 하드디스크가 접속된 IDE 버스와 인터페이스하는 IDE인터페이스부(140)로 구성된다.

도 2는 본 발명에 따른 이중버스를 연결하는 고기밀 호스트어댑터의 상세블록 구성도로서, 시스템 메모리 또는 중앙처리장치(CPU)와 접속되어 데이터를 인터페이스하는 PCI 버스와 IDE방식의 하드디스크의 데이터를 인터페이스하는 IDE버스간의 데이터를 제공된 비밀키에 의하여 암호화 또는 복호화하는 이중버스 고기밀 어댑터(100)와, 이중버스 고기밀 어댑터(100)에 비밀키 데이터를 저장하고 이를 제공하는 롬바이오스(ROM BIOS)(200)로 크게 구성된다.

여기서, 이중버스 고기밀 어댑터(100)는 ATAPI(AT Attachment with Packet Interface) 방식의 RAID(Redundant Array with Inexpensive Disks) 컨트롤러를 사용한다.

또한, 이중버스 고기밀 어댑터(100)는 PCI 버스에 접속되어 데이터를 인터페이스하도록 마스터컨트롤러(111)와 슬레이브컨트롤러(112)로 구성된 PCI인터페이스부(112)와, 상기 마스터컨트롤러(111)를 통하여 하드디스크로 전송되는 데이터를 쓰기/읽기에 따라 제공된 비밀키 데이터에 의하여 암호화/복호화하는 제 1 암/복호화부(121), 상기 제 1 암/복호화부(121) 및 제 2 암/복호화부(131)로부터 입출력되는 데이터를 선입선출 버퍼링(First Input First Output buffering)하는 선입선출버퍼(FIFO)(122)와, 상기 선입선출버퍼(122)를 통해 선입선출되는 데이터를 하드디스크로의 쓰기/읽기 동작에 따라 암호화/복호화하여 IDE 버스로 전송하는 제 2 암/복호화부(131)와, 상기 제 2 암/복호화부(131)와 IDE 버스에 접속하여 데이터를 인터페이스하는 IDE인터페이스부(140)와, 상기 제 1, 제 2 암/복호화부(121)(131)의 암호화 또는 복호화를 결정하여 인에이블시킴과 아울러 암호화 및 복호화할 비밀키 데이터를 제공하는 암/복호화제어부(150)와, 롬바이오스(200)에 저장된 비밀키 데이터를 상기 암/복호화제어부(150)에 전송하는 롬인터페이스(162)와, 상기 슬레이브컨트롤러(112)를 통하여 PCI 환경을 설정하고 호스트에서 엑세스할 수 있도록 환경정보의 저장 인터페이스를 수행하는 PCI버스 환경인터페이스부(Configuration Interface)와, PCI버스에 인가된 정보를 슬레이브컨트롤러(112)를 통하여 입출력 스페이스 인터페이스부(IO Space Interface)와, DMA(Data Memory Access) 동작에 필요한 각종 파라미터들을 호스트로부터 PCI 슬레이브컨트롤러(112)를 통하여 저장하는 DMA저장부(DMA Register)로 구성된다.

또한, 암/복호화제어부(150)는 제 1, 제 2 암/복호화부(121)(131)에 현재 입력된 데이터의 암호화/복호화 여부를 접속 요청자의 인증여부에 따라 결정함과 아울러 해당 비밀키 데이터를 저장 및 제공하는 비밀키 제어부(152)와, 상기 비밀키 제어부(152)로부터 전송된 비밀키 데이터와 제 1, 제 2 암/복호화부(121)(131)의 제어신호에 따라 해당 암/복호화부(121)(131)를 인에이블 시킴과 아울러 비밀키 데이터를 제공하는 제 1, 제 2 암/복호화 구동부(151)(153)로 구성된다.

이와 같이 구성된 본 발명의 실시예에 따른 작용을 첨부된 도 1, 도 2를 참조하여 보다 상세히 설명하면 다음과 같다.

먼저, 본 발명은 고기밀 저장장치로서, 정보를 저장한 사용자의 비밀키를 이용하여 복호화하고 이를 다시 정보 제공을 요청한 사용자의 비밀키를 이용하여 암호화하므로 정보 요청자만이 볼 수 있는 형태로 정보를 읽어내게 된다.

즉, 컴퓨터 내에 내장된 정보를 외부로 전송시 내장된 정보를 정보 소유자의 비밀키로 복호화하고 복호화된 정보를 정보 요구자의 비밀키로 재 암호화하여 제공한다. 이와 반대로 외부 접근자가 정보를 컴퓨터 내에 저장하려할 때에는 암호화하여 전송되어진 정보를 정보 전송자의 키로 복호화하고 복호화된 정보를 컴퓨터 소유자의 비밀키로 암호화하여 저장하게 된다.

또한 개인용, 산업용 컴퓨터의 이중 입출력버스(IO Bus)(PCI, SCSI, IDE, ISA, USB, Firewire(IEEE1394,

iLink), RS232 등) 구조간의 상호 연결하도록 한 것이다.

이중 입출력버스는 SCSI와 IDE, PCI와 SCSI, 그리고, PCI와 USB 또는 Firewire 등의 이중버스간의 연결에서 암호화 하드웨어 모듈 2개와 레지스터 1개를 어댑터에 내장하여 컴퓨터 메인버스를 점유하지않고 컴퓨터 소유자의 키와 정보 요구자의 키를 이용하여 암호화와 복호화를 어댑터 내부에서 동시에 처리할 수 있도록 한 것이다.

본 발명의 바람직한 실시예로서, 이중 버스간의 고속연결을 기본으로 하는 기술이므로 컴퓨터 내부 버스 중에서 고속이면서도 가장 널리 사용되는 PCI 버스와 저장장치용 IDE 버스를 사용한다.

도 1은 본 발명의 실시예에 따른 이중버스를 연결하는 고기밀 호스트어댑터를 설명하기 위한 개략 구성도로서, PCI 버스 인터페이스(110)을 통해 외부 접근자가 IDE 버스에 접속된 하드디스크에 저장된 정보를 액세스할 경우, 제 2 암호화/복호화처리장치(130)에서 하드디스크에 저장된 정보를 정보 소유자의 비밀키(Key2)로 복호화하고, 복호화된 정보를 제 1 암호화/복호화처리장치(120)에서 정보 요구자의 비밀키(Key1)로 재 암호화한 후 PCI 인터페이스부(110)를 통해 외부 접근자에게 전송한다.

반대로, 외부 접근자가 정보를 하드디스크에 저장하려 할 때는 PCI 버스 인터페이스부(110)를 통해 암호화하여 전송된 데이터를 제 1 암호화/복호화 처리장치(120)에서 제공된 비밀키(Key1)로 복호화하고, 복호화된 데이터는 제 2 암호화/복호화 처리장치(130)에서 컴퓨터 소유자의 비밀키(Key2)로 암호화한 후 IDE 인터페이스부(140)를 통하여 하드디스크의 해당 영역에 저장한다.

도 2는 본 발명의 실시예에 따른 이중버스를 연결하는 고기밀 호스트어댑터의 상세 블록도로서, 먼저, 고기밀 호스트어댑터(100)에 내장된 PCI환경정보 인터페이스부(Configuration Interface)는 슬레이브 컨트롤러(110)를 통해 필요한 PCI 환경 정보를 제공받아 PCI 버스 제어를 위한 환경을 설정하고 호스트에서 액세스할 수 있도록 하기 위하여 PCI 환경을 저장한다.

PCI 버스에 인가된 데이터는 마스터 컨트롤러(111)와 슬레이브 컨트롤러(112)를 통해 해당 장치로 전송된다.

여기서, 데이터 저장방식에 따라 몇 가지 저장경로가 있는데, 먼저 정보가 슬레이브 컨트롤러(112)를 통해 입출력 스페이스 인터페이스(IO Space interface)에서 IDE 채널로 연결되는 PIO(Process Input Output) 모드이며, 이 방식은 DMA 컨트롤러를 이요하지 않고 호스트 중앙처리장치가 직저 데이터를 전송하여 저장하는 방식이다.

다른 경로는 마스터 컨트롤러(111)에서 선입선출버퍼(122)로 이어지는 MDMA(Multi work Direct Memory Access)방식과 UDMA(Ultra Direct Memory Access)방식이 있다. DMA 동작에 필요한 각종 파라미터들은 호스트로부터 PCI 슬레이브 컨트롤러(122)를 통하여 DMA 저장부(DMA Register)에 저장된다.

제 1, 제 2 암/복호화부(121)(131)는 3-DES로, 일단 PCI 버스의 마스터 컨트롤러(111)또는 슬레이브 컨트롤러(112)를 통해 각 디바이스 내부로 전달된 정보는 컴퓨터 부팅(booting)인지 또는 외부 접근자의 접근에 의한 것인지를 확인한 후 접근된 방식을 비밀키 제어부(152)에 저장한다. 비밀키 제어부(152)는 외부 접근자의 비밀키를 확인하여 정보를 공유할 수 있는지를 인증한 후 공유가 가능한 접근자이면 롬 바이오스(200)에 등록된 컴퓨터 소유자의 비밀키를 롬인터페이스부(162)를 통해 전송받아 저장한다.

만약 컴퓨터 소유자가 하드디스크에 데이터를 저장할 때 자신의 비밀키로 저장하였다면 외부 접근자가 하드디스크에 내장된 데이터를 읽기 요청 전에 외부 접근자는 기 설정된 비밀키와 비교하여 정보접근 가능자임을 인증받는다.

이와 같이 인증절차를 통해 인증받은 외부 접근자가 하드디스크에 저장된 필요한 정보를 액세스하고자 할 경우에 대하여 설명하면 다음과 같다.

먼저, 하드디스크에 저장된 데이터를 전송하기에 앞서, 해당 데이터의 암호화/복호화를 해야 한다. 즉, 이를 위해 데이터의 암호화/복호화에 대한 제어정보와 비밀키 정보를 PCI 슬레이브 컨트롤러(112)를 통해 비밀키 제어부(152)에 전송한다.

비밀키 제어부(152)는 암호화/복호화에 대한 제어정보와 비밀키를 참조하여 제 1, 제 2 암/복호화 구동부(151)(153)를 통해 각각 제 1, 제 2 암/복호화부(121)(131)를 구동시키게 된다.

이때, 제 1, 제 2 암/복호화구동부(151)(153)는 해당 암/복호화부(121)(131)를 인에이블 시킴과 아울러 입력된 데이터를 암호화할 것인지, 복호화할 것인지를 결정하여 구동시킨다. 더불어서, 전송된 비밀키를 해당 암/복호화부(121)(131)에 제공한다.

PCI 버스의 슬레이브 컨트롤러(112)를 통하여 하드디스크에 읽기 명령을 전달하면, 하드디스크에 암호화된 데이터가 IDE 버스를 통해 채널 인터페이스(140)(MDMA, UDMA) 또는 IO 스페이스 인터페이스(IO Space Interface)를 통하여 제 2 암/복호화부(131)에 전송된다.

제 2 암/복호화부(131)에서는 제 2 암/복호화구동부(153)를 통해 기 설정된 비밀키에 대하여 암호화 또는 복호화한 후 선입선출버퍼(122)에 입력한다.

선입선출버퍼(122)에서는 복호화하여 입력된 데이터를 선입선출 버퍼링하여 제 1 암/복호화부(121)로 데이터를 전송한다.

제 1 암/복호화부(121)는 선입선출버퍼(122)를 통해 입력된 복호화된 데이터를 제공받은 접근자 비밀키에 의하여 다시한번 암호화한 후 마스터컨트롤러(111)를 통해 PCI 버스로 전송되고, PCI 버스를 통하여 시스템 메모리로 전송하게 된다.

만약, 만약 접속자가 IDE 버스에 접속된 하드디스크에 데이터를 저장하고자 할 경우에는 읽는 경우와 반대방향으로 데이터가 처리된다.

즉, 마스터 컨트롤러(111)를 통해 저장이 요청된 암호화된 데이터는 제 1 암/복호화부(121)에 전달되어

제 1 암/복호화 구동부(151)에서 제공된 비밀키에 의하여 복호화한다. 복호화된 데이터는 선입선출버퍼(122)를 통하여 제 2 암/복호화부(131)로 전송되고, 전송된 데이터는 제 2 암/복호화구동부(131)의 제어에 의하여 롬바이오스(200)에서 제공된 비밀키로 암호화한 후 해당 채널(140)을 통하여 해당 하드디스크 영역에 저장하게 된다.

즉, 하드디스크로의 읽기동작은 복호화과정을 거치며, 쓰기동작은 암호화과정을 거치게 된다.

이때, 만약 정보 접근자가 입력한 비밀키가 암/복호화에 사용한 비밀키와 비교하여 다를 경우에는 하드디스크로부터의 데이터를 읽을 수 없으며, 그로 인해 하드디스크에 저장된 데이터를 보호할 수 있게된다.

본 발명에 따른 바람직한 실시예에 대해 설명하였으나, 이종버스로서 PCI 버스와 IDE 버스 뿐만아니라, SCSI 또는 ISA, USB, Firewire, RS232등 상호간에도 적용이 가능하며, 본 기술분야에서 통상의 지식을 가진자라면 본 발명의 특허청구범위를 벗어남이 없이 다양한 변형예 및 수정예를 실시할 수 있을 것으로 이해된다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 따른 이종버스를 연결하는 고기밀 호스트어댑터는 외부 접근자가 인증된 정보 요구자로 가장하고 정보를 요구하여 충실하게 정보를 전달 받더라도 암호화 모듈이나 이와 상응하는 프로그램을 구비하거나 만들어야 하므로 외부로의 정보 유출이 불가능한 효과가 있다. 또한, 데이터를 암호화하여 하드디스크에 저장하므로 하드디스크를 도난, 유실 또는 탈취되어도 비밀키를 알지못하면 하드디스크에 저장된 데이터를 판독할 수 없는 효과가 있다. 또한, 암호화 하드웨어모듈 2개와 선입선출버퍼 1개를 내장하여 데이터를 처리하도록 하여 컴퓨터의 메인버스를 점유하지 않아도 되므로 메인버스의 부하를 줄일 수 있어 처리속도를 향상시키는 효과가 있다.

(57) 청구의 범위

청구항 1

컴퓨터의 시스템 메모리 또는 중앙처리장치와 인터페이스하는 제 1 버스와, 하드디스크의 데이터의 읽기/쓰기를 수행하는 상기 제 1 버스와 다른 방식의 제 2 버스와, 상기 제 1 버스와 제 2 버스 간의 데이터를 인터페이스하는 어댑터와, 상기 어댑터의 동작제어를 위한 프로그램이 등록된 롬바이오스로 구성된 이종버스간의 어댑터에 있어서,

상기 제 1 버스에 접속된 마스터컨트롤러와 하드디스크간에 전송되는 데이터를 쓰기/읽기에 따라 제공된 비밀키 데이터에 의하여 암호화/복호화하는 제 1 암/복호화수단;

상기 제 1 암/복호화수단 및 다른 암/복화수단으로부터 입출력되는 데이터를 선입선출 버퍼링하는 선입선출버퍼;

상기 선입선출버퍼를 통해 선입선출되는 데이터를 하드디스크로의 쓰기/읽기 동작에 따라 암호화/복호화하여 제 2 버스로 전송하는 제 2 암호화/복호화수단;

상기 제 1, 제 2 암/복호화수단의 암호화 또는 복호화를 결정하여 인에이블시킴과 아울러 암호화 및 복호화할 비밀키 데이터를 제공하는 암/복호화제어수단을 포함하여 이루어짐을 특징으로 하는 이종버스를 연결하는 고기밀 호스트어댑터.

청구항 2

제 1 항에 있어서, 상기 제 1, 제 2 암/복호화수단은 하드디스크로부터 데이터를 읽어올 경우에는 복호화과정을 수행하며, 하드디스크에 데이터를 기록할 경우에는 암호화과정을 수행함을 특징으로 하는 이종버스를 연결하는 고기밀 호스트어댑터.

청구항 3

제 1 항 또는 제 2 항에 있어서, 상기 제 1, 제 2 암/복호화수단은 암호화된 데이터가 입력되면 제공된 비밀키 데이터에 의하여 복호화하고, 복호화된 데이터가 입력되면 제공된 비밀키 데이터에 의하여 암호화함을 특징으로 하는 이종버스를 연결하는 고기밀 호스트어댑터.

청구항 4

제 1 항에 있어서, 상기 제 1 암/복호화수단에서 암호화/복호화된 데이터는 상기 마스터컨트롤러가 접속된 제 1 버스를 통해 시스템 메모리로 전송함을 특징으로 하는 이종버스를 연결하는 고기밀 호스트어댑터.

청구항 5

제 1 항 또는 제 4 항에 있어서, 상기 제 1 버스는 PCI 방식의 버스이고, 제 2 버스는 IDE방식 또는 SCSI 방식 중 하나의 버스임을 특징으로 하는 이종버스를 연결하는 고기밀 호스트어댑터.

청구항 6

제 1 항에 있어서, 상기 암/복호화제어수단은 상기 제 1, 제 2 암/복호화수단에 현재 입력된 데이터의 암호화/복호화 여부를 접속 요청자의 인증여부에 따라 결정함과 아울러 해당 비밀키 데이터를 저장 및 제공하는 비밀키 제어수단; 및

상기 비밀키 제어수단으로부터 전송된 비밀키 데이터와 제 1, 제 2 암/복호화수단 제어신호에 따라 해당 암/복호화수단을 인에이블 시킴과 아울러 비밀키 데이터를 제공하는 제 1, 제 2 암/복호화 구동수단을 포

합하여 구성된 것을 특징으로 하는 이중버스를 연결하는 고기밀 호스트어댑터.

청구항 7

제 6 항에 있어서, 상기 비밀키 제어수단에 제공되는 비밀키 데이터는 상기 제 1 버스에 접속된 슬레이브 컨트롤러를 통해 전송된 접속인증 요청자의 비밀키 데이터와 롬바이오스에 저장된 비밀키를 비교한 결과에 따라 해당 하드디스크의 접근을 허여함을 특징으로 하는 이중버스를 연결하는 고기밀 호스트어댑터.

청구항 8

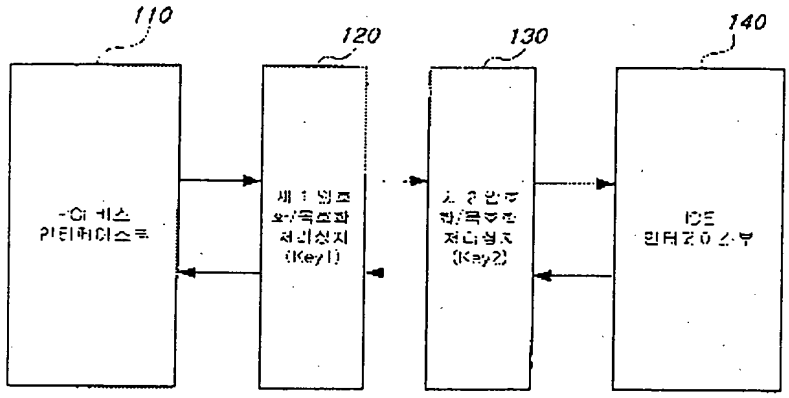
제 6 항 또는 제 7 항에 있어서, 상기 제 1 암/복호화수단에 제공되는 비밀키는 현재 하드디스크에 직접 엑세스하고 있는 접근자가 제공하는 제 1 비밀키이고, 제 2 암/복호화수단에 제공되는 비밀키는 네트워크를 통하여 현재 하드디스크를 엑세스하는 접근자가 제공하는 제 2 비밀키임을 특징으로 하는 이중버스를 연결하는 고기밀 호스트어댑터.

청구항 9

제 6 항에 있어서, 상기 제 1, 제 2 암/복호화수단의 암호화모듈로 3-데이터암호화시스템(Triple Data Encryption System)을 내장함을 특징으로 하는 이중버스를 연결하는 고기밀 호스트어댑터.

도면

도면1



도면2